

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002104

International filing date: 04 February 2005 (04.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-029928
Filing date: 05 February 2004 (05.02.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

04. 2. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 5 日
Date of Application:

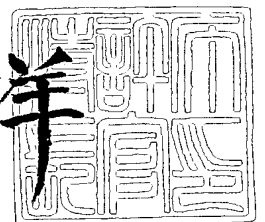
出 願 番 号 特 願 2 0 0 4 - 0 2 9 9 2 8
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 0 2 9 9 2 8]

出 願 人 ト レ ン ド マ イ ク ロ 株 式 会 社
Applicant(s):

2 0 0 5 年 3 月 1 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 84026
【提出日】 平成16年 2月 5日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 9/00
H04B 17/00

【発明者】
【住所又は居所】 東京都渋谷区代々木 2 - 1 - 1 トレンドマイクロ株式会社内
【氏名】 近藤 賢志

【発明者】
【住所又は居所】 東京都渋谷区代々木 2 - 1 - 1 トレンドマイクロ株式会社内
【氏名】 矢田部 茂

【特許出願人】
【識別番号】 397011166
【氏名又は名称】 トレンドマイクロ株式会社

【代理人】
【識別番号】 100098084
【弁理士】
【氏名又は名称】 川▲崎▼ 研二

【選任した代理人】
【識別番号】 100111763
【弁理士】
【氏名又は名称】 松本 隆

【手数料の表示】
【予納台帳番号】 038265
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、

前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、

前記判定手段による判定結果を出力する出力手段と
を備えることを特徴とする受信装置。

【請求項 2】

受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、

前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、

前記判定手段により実行が許可された場合に前記プログラムを実行する実行手段と
を備えることを特徴とする受信装置。

【請求項 3】

受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、

前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、

前記判定手段により実行が許可されなかった場合に、使用可能な機能を制限して前記プログラムを実行するか否かを問い合わせるメッセージを出力する出力手段と、

操作手段と、

前記出力手段によるメッセージの出力に応じて前記操作手段から前記プログラムを実行する旨が指示された場合に、前記プログラムを実行する実行手段と、

前記実行手段により実行されたプログラムにおいて使用可能な機能を、前記登録手段に登録された情報に従って制限する制限手段と

を備えることを特徴とする受信装置。

【請求項 4】

前記判定手段は、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されていない場合に、前記プログラムの実行を許可する

ことを特徴とする請求項 2 または 3 に記載の受信装置。

【請求項 5】

前記登録手段には、受信したプログラムにおいて使用することが許可された関数を示す情報、または前記プログラムにおいて使用することが禁止された関数を示す情報が登録され、

前記機能情報は、前記受信手段により受信されたプログラムに含まれている関数を示す情報である

ことを特徴とする請求項 1 ～ 3 のいずれかに記載の受信装置。

【請求項 6】

前記登録手段には、受信したプログラムに従ってアクセスすることが許可されたリソースを示す情報、または前記プログラムに従ってアクセスすることが禁止されたリソースを

示す情報が登録され、

前記機能情報は、前記受信手段により受信されたプログラムに従ってアクセスされるリソースを示す情報である

ことを特徴とする請求項 1 ～ 3 のいずれかに記載の受信装置。

【請求項 7】

受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第 1 の受信手段と、

前記第 1 の受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記プログラムの受信可否を判定する判定手段と、

前記判定手段により受信が許可された場合に前記プログラムを受信する第 2 の受信手段と、

前記第 2 の受信手段により受信されたプログラムを実行する実行手段と

を備えることを特徴とする受信装置。

【請求項 8】

ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、

前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの中継可否を判定する判定手段と、

前記判定手段により中継が許可された場合に、前記受信手段により受信された宛先情報によって示される送信先へ前記プログラムを送信する送信手段と

を備えることを特徴とする中継装置。

【請求項 9】

前記判定手段は、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されていない場合に、前記プログラムの中継を許可する

ことを特徴とする請求項 8 に記載の中継装置。

【請求項 10】

ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、

前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、

前記判定手段による判定結果と前記プログラムを、前記受信手段により受信された宛先情報によって示される送信先へ送信する送信手段と

を備えることを特徴とする中継装置。

【請求項 11】

前記登録手段には、ネットワークを介して提供されるプログラムにおいて使用することが許可された関数を示す情報、または前記プログラムにおいて使用することが禁止された関数を示す情報が登録され、

前記機能情報は、前記受信手段により受信されたプログラムに含まれている関数を示す情報である

ことを特徴とする請求項 8 または 10 に記載の中継装置。

【請求項 12】

前記登録手段には、ネットワークを介して提供されるプログラムに従ってアクセスすることが許可されたりソースを示す情報、または前記プログラムに従ってアクセスすることが禁止されたりソースを示す情報が登録され、

前記機能情報は、前記受信手段により受信されたプログラムに従ってアクセスされるリソースを示す情報である

ことを特徴とする請求項 8 または 10 に記載の中継装置。

【請求項 13】

コンピュータに、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する第 1 のステップと、

予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第 1 のステップにて受信された機能情報とを比較して、使用することの許可されていない機能が前記第 1 のステップにて受信されたプログラムにおいて使用されているか否かを判定する第 2 のステップと、

前記第 2 のステップにて判定された判定結果を出力する第 3 のステップと

を実行させるためのプログラム。

【請求項 14】

コンピュータに、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する第 1 のステップと、

予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第 1 のステップにて受信された機能情報とを比較して、前記第 1 のステップにて受信されたプログラムの実行可否を判定する第 2 のステップと、

前記第 2 のステップにて実行が許可された場合に前記プログラムを実行する第 3 のステップと

を実行させるためのプログラム。

【請求項 15】

コンピュータに、

プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第 1 のステップと、

予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第 1 のステップにて受信された機能情報とを比較して、前記機能情報と対応付けられたプログラムの受信可否を判定する第 2 のステップと、

前記第 2 のステップにて受信が許可された場合に前記プログラムを受信する第 3 のステップと、

前記第 3 のステップにて受信されたプログラムを実行する第 4 のステップと

を実行させるためのプログラム。

【請求項 16】

コンピュータに、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する第 1 のステップと、

予めメモリに登録された、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第 1 のステップにて受信された機能情報とを比較して、前記第 1 のステップにて受信されたプログラムの中継可否を判定する第 2 のステップと、

前記第 2 のステップにて中継が許可された場合に、前記第 1 のステップにて受信された

宛先情報によって示される送信先へ前記プログラムを送信する第 3 のステップと
を実行させるためのプログラム。

【請求項 1 7】

コンピュータに、

プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する第 1 のステップと、

予めメモリに登録された、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第 1 のステップにて受信された機能情報とを比較して、使用することの許可されていない機能が前記第 1 のステップにて受信されたプログラムにおいて使用されているか否かを判定する第 2 のステップと、

前記第 2 のステップにて判定された判定結果と前記プログラムを、前記第 1 のステップにて受信された宛先情報によって示される送信先へ送信する第 3 のステップと
を実行させるためのプログラム。

【請求項 1 8】

請求項 1 3 ～ 1 7 のいずれかに記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】 明細書

【発明の名称】 情報機器上および伝送経路上でのプログラム分析によるセキュリティの確保

【技術分野】

【0001】

本発明は、情報機器のセキュリティを確保するための技術に関する。

【背景技術】

【0002】

インターネット等のオープンネットワークでは、様々な人々が自由に情報の公開やプログラムの提供を行うことができる。このため、通信端末に記憶されている個人情報を読み出して通信端末の外部へ密かに送信してしまうプログラム等、通信端末において実行させると、セキュリティ上、問題のあるプログラムがオープンネットワークを介して通信端末に提供されてしまう場合がある。このようなプログラムによって引き起こされる問題から通信端末を保護するため、例えば、特許文献1に記載されたプログラム実行装置では、信頼できるプログラム発信元を示す識別情報（例えば、IPアドレスやURL）をメモリに登録しておき、ネットワークを介して受信したプログラムについては、このプログラムの発信元を示す識別情報がメモリに登録されている場合にのみ、プログラムの実行を許可するようにしている。

【特許文献1】 特開2001-117769号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

ところで、特許文献1に記載された技術では、信頼できる全てのプログラム発信元の識別情報をメモリに登録しておかなければならない。したがって、信頼できるプログラム発信元の追加や削除に応じて、メモリに登録されている識別情報を頻繁に更新しなければならず煩雑である。また、インターネットのような大規模なネットワークでは、信頼できるプログラム発信元が極めて多数存在するから、これらの識別情報を漏れなく登録しておくことは実質的に困難である。また、仮に、信頼できる全てのプログラム発信元の識別情報をメモリに登録できたとしても、この場合には、識別情報を登録しておくために必要となるメモリ容量が極めて大きなものになってしまうから、特に、携帯電話機等の小型の通信端末においては、メモリの容量を増やさなければならない等、コストアップを招いてしまう。

【0004】

一方で、例えば、通信端末において、ネットワークを介して受信したプログラムの内容を解析し、このプログラムを実行した場合にセキュリティ上の問題が起きないか検証しようとする、通信端末に高い演算能力が備わっていなければならない。加えて、このような検証処理は負荷が大きく時間もかかる。また、ネットワーク上に設けられたサーバ等の中継装置において、通信端末へ転送するプログラムの内容を解析し、このプログラムを通信端末において実行した場合にセキュリティ上の問題が起きないか検証しようとする、中継装置に高い演算能力が備わっていなければ、通信の遅延を招いたり、通信網のトラフィックに支障をきたしてしまう。

【0005】

本発明は、以上説明した事情に鑑みてなされたものであり、その目的は、ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定できるようにすることである。

【課題を解決するための手段】

【0006】

上記課題を解決するために、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能

を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、前記判定手段による判定結果を出力する出力手段とを備える受信装置を提供する。

【0007】

また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。このプログラムは、コンピュータのメモリに予めインストールされていてもよいし、ネットワークを介した通信や、上記記録媒体を介してコンピュータにインストールされてもよい。

【0008】

本発明によれば、受信装置は、使用することの許可されていない機能が、受信したプログラムにおいて使用されているか否かを、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定し、判定結果を出力する。

【0009】

また、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、前記判定手段により実行が許可された場合に前記プログラムを実行する実行手段とを備える受信装置を提供する。また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【0010】

本発明によれば、受信装置は、受信したプログラムの実行可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。

【0011】

また、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第1の受信手段と、前記第1の受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記プログラムの受信可否を判定する判定手段と、前記判定手段により受信が許可された場合に前記プログラムを受信する第2の受信手段と、前記第2の受信手段により受信されたプログラムを実行する実行手段とを備える受信装置を提供する。また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【0012】

本発明によれば、受信装置は、プログラムの受信可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。

【0013】

また、本発明は、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの中継可否を判定する判定手段と、前記判定手段により中継が許可された場合に、前記受信手段により受信された宛先情報によって示される送信先へ前記プログラムを送信する送信手段とを備える中継装置を提供する。

【0014】

また、本発明は、上記中継装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。このプログラムは、コンピュータのメモリに予めインストールされていてもよいし、ネットワークを介した通信や、上記記録媒体を介してコンピュータにインストールされてもよい。

【0015】

本発明によれば、中継装置は、受信したプログラムの中継可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。

【0016】

また、本発明は、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、前記判定手段による判定結果と前記プログラムを、前記受信手段により受信された宛先情報によって示される送信先へ送信する送信手段とを備える中継装置を提供する。また、本発明は、上記中継装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【0017】

本発明によれば、中継装置は、使用することの許可されていない機能が、受信したプログラムにおいて使用されているか否かを、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定し、判定結果をプログラムとともに送信する。

【発明の効果】

【0018】

本発明によれば、ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定することができる。

【発明を実施するための最良の形態】

【0019】

以下、図面を参照して本発明の実施形態について説明する。

[A. 第1実施形態]

図1は、第1実施形態に係る通信システム1の構成を例示するブロック図である。同図において、コンテンツプロバイダ10は、携帯電話機50にコンテンツを提供する事業者である。コンテンツサーバ10aは、インターネット30および移動パケット通信網40を介して携帯電話機50とパケット通信を行うことができる。このコンテンツサーバ10aには、携帯電話機50用のプログラムと、このプログラムを検査機関20において検査した結果得られる検査結果データ202とが記憶されている。なお、コンテンツサーバ10aに記憶されているプログラムは、プログラムの実行時に使用される画像データや音声データ等を含んだソフトウェアであってもよい。

【0020】

検査機関20は、携帯電話機50に提供されるプログラムをコンテンツプロバイダ10からの検査依頼に応じて検査する機関であり、プログラム検査装置20aには安全性評価表201が記憶されている。この安全性評価表201には、携帯電話機50用のプログラムに含まれている、ファンクションコール、システムコール、機能呼び出し等の各種の関数のうち、ネットワークを介して提供されるプログラムに含まれていた場合、このプログラムを実行すると携帯電話機50においてセキュリティ上の問題が起きる可能性のある関数の一覧が記録されている。加えて、この安全性評価表201には、携帯電話機50がアクセスすることのできる各種のリソースのうち、ネットワークを介して提供されるプロ

ラムに従ってアクセスされると、携帯電話機50においてセキュリティ上の問題が起きる可能性のあるリソースの一覧が記録されている。

【0021】

プログラム検査装置20aは、安全性評価表201を用いて検査対象となるプログラムを解析し、検査対象となるプログラムから安全性評価表201に記録されている関数を抽出する。加えて、プログラム検査装置20aは、検査対象となるプログラムを実行した場合にアクセスされるリソースのうち、安全性評価表201に記録されているリソースを特定する。そして、プログラム検査装置20aは、抽出した関数の名称や、特定したリソースを示す情報（例えば、リソースの格納場所を示すURLやパス、リソースに割り当てられた識別名等）を収めた検査結果データ202を生成する。この検査結果データ202がコンテンツプロバイダ10へと返却され、プログラムに付与されてコンテンツサーバ10aに記憶される。

【0022】

なお、プログラム検査装置20aは、検査対象となるプログラムに含まれている全ての関数や、検査対象となるプログラムを実行した場合にアクセスされる全てのリソースを検査結果データ202に記録する構成であってもよい。

【0023】

携帯電話機50は、移動パケット通信網40に收容される通信端末（受信装置）であって、コンテンツサーバ10aからプログラムをダウンロードしてこれを実行することができる。

【0024】

次に、図2は、検査結果データ202のデータ構成を例示する図である。同図に示すように、検査結果データ202には、検査されたプログラムのファイル名と、このプログラムのハッシュ値を算出するために用いたハッシュアルゴリズムの名称と、算出されたハッシュ値とが記録されている。加えて、この検査結果データ202には、安全性評価表201を用いて検査対象となるプログラムを解析した結果得られた、このプログラムに含まれている関数の名称の一覧や、このプログラムを実行した場合にアクセスされるリソースを示す情報の一覧が記録されている。なお、検査結果データ202に記録されたハッシュ値は、プログラム検査装置20aによる検査後にプログラムがすり替えられたり改竄されていないことを携帯電話機50において検証するために用いられる。

【0025】

図3は、携帯電話機50のハードウェア構成を例示するブロック図である。同図において、CPU501は、ROM502や不揮発性メモリ507に記憶されている各種のプログラムを実行することにより携帯電話機50の各部を制御する。ROM502には、携帯電話機50を制御するためのプログラム等が記憶されている。RAM503は、CPU501のワークエリアとして用いられる。無線通信部504は、CPU501の制御の下、移動パケット通信網40の基地局（図示を省略）との間で行われる無線通信を制御する。操作入力部505は、複数のキーを有しており、これらのキーの操作に応じた操作信号をCPU501に出力する。液晶表示部506は、液晶表示パネルと、この液晶表示パネルの表示制御を行う駆動回路とを有している。

【0026】

不揮発性メモリ507には、例えば、携帯電話機50のオペレーティングシステムやWW（World Wide Web）ブラウザ用のソフトウェアが記憶されている。また、この不揮発性メモリ507に、コンテンツサーバ10aからダウンロードされたプログラムとその検査結果データ202が記憶される。また、不揮発性メモリ507には、セキュリティ管理テーブル507aが記憶されている。

【0027】

セキュリティ管理テーブル507aには、図4に示すように、携帯電話機50用のプログラムに含まれている各種の関数のうち、ネットワークを介して受信したプログラムを実行する場合に使用することが許可された関数の名称や、逆に、ネットワークを介して受信

したプログラムを実行する場合に使用することが禁止された関数の名称が登録されている。加えて、このセキュリティ管理テーブル 5 0 7 a には、携帯電話機 5 0 がアクセスすることのできる各種のリソースのうち、ネットワークを介して受信したプログラムを実行する場合にアクセスすることが許可されたリソースを示す情報や、逆に、ネットワークを介して受信したプログラムを実行する場合にアクセスすることが禁止されたリソースを示す情報が登録されている。また、プログラムの実行可否をユーザに問い合わせる関数やリソースについては、セキュリティ管理テーブル 5 0 7 a において「許否」の項目に“ユーザ確認”が登録されている。

【0 0 2 8】

不揮発性メモリ 5 0 7 には、携帯電話機 5 0 に対して設定可能な各セキュリティレベル毎に、例えば、“レベル 1”用のセキュリティ管理テーブル 5 0 7 a や、“レベル 2”用のセキュリティ管理テーブル 5 0 7 a 等、複数のセキュリティ管理テーブル 5 0 7 a が記憶されている。携帯電話機 5 0 において、ネットワークを介して受信したプログラムの実行可否を判定する際には、上述した複数のセキュリティ管理テーブル 5 0 7 a の中から、現時点において携帯電話機 5 0 に設定されているセキュリティレベルに対応するセキュリティ管理テーブル 5 0 7 a が用いられる。また、セキュリティレベルは、携帯電話機 5 0 のユーザによって設定される。

【0 0 2 9】

なお、セキュリティ管理テーブル 5 0 7 a に登録する関数や、各関数についての使用の許否は、携帯電話機 5 0 のユーザが任意に変更できる構成であってもよい。これはセキュリティ管理テーブル 5 0 7 a に登録するリソースや、各リソースについてのアクセスの許否についても同様である。

【0 0 3 0】

次に、第 1 実施形態の動作について説明する。

図 5 は、プログラムとその検査結果データ 2 0 2 が携帯電話機 5 0 にダウンロードされるまでの通信システム 1 各部の動作について例示するシーケンスチャートである。同図に示すように、例えば、コンテンツプロバイダ 1 0 によって作成された携帯電話機 5 0 用のプログラムは、検査依頼要求とともにコンテンツサーバ 1 0 a からプログラム検査装置 2 0 a へと送信される（ステップ S 1 0 1）。

【0 0 3 1】

プログラム検査装置 2 0 a は、プログラムおよび検査依頼要求を受信すると、受信したプログラムを解析する（ステップ S 1 0 2）。プログラム検査装置 2 0 a は、受信したプログラムから安全性評価表 2 0 1 に記録されている関数を抽出するとともに、受信したプログラムを実行した場合にアクセスされるリソースのうち、安全性評価表 2 0 1 に記録されているリソースを特定する。また、プログラム検査装置 2 0 a は、任意のハッシュアルゴリズムを用いて、受信したプログラムのハッシュ値を算出する。そして、プログラム検査装置 2 0 a は、抽出した関数の名称や、特定したリソースを示す情報に加え、算出したハッシュ値や、使用したハッシュアルゴリズムの名称、受信したプログラムのファイル名等を収めた検査結果データ 2 0 2 を生成する（ステップ S 1 0 3）。

【0 0 3 2】

また、プログラム検査装置 2 0 a は、生成した検査結果データ 2 0 2 に電子署名を施す（ステップ S 1 0 4）。この電子署名は、プログラム検査装置 2 0 a によって生成された検査結果データ 2 0 2 が、すり替えられたり改竄されていないことを携帯電話機 5 0 において検証するために用いられる。この後、プログラム検査装置 2 0 a は、電子署名が施された検査結果データ 2 0 2 をコンテンツサーバ 1 0 a へ返信する（ステップ S 1 0 5）。コンテンツサーバ 1 0 a は、検査結果データ 2 0 2 を受信すると、この検査結果データ 2 0 2 を、検査対象となったプログラムに付加してメモリに記憶し（ステップ S 1 0 6）、プログラムとその検査結果データ 2 0 2 を携帯電話機 5 0 からダウンロード可能な状態とする。

【0 0 3 3】

一方、携帯電話機 50 では、まず、セキュリティレベルを設定する処理が行われる（ステップ S107）。このセキュリティレベルの設定に際しては、例えば、図 6 に示すような画像が液晶画面に表示され、ユーザは、操作入力部 505 を操作して、携帯電話機 50 に設定するセキュリティレベルを“レベル 0（なし）”～“レベル 5”の中から任意に選択することができる。また、ユーザによって設定されたセキュリティレベルの値は、不揮発性メモリ 507 に記憶される。

【0034】

この後、コンテンツサーバ 10a からプログラムをダウンロードする際には、まず、携帯電話機 50 において WWW ブラウザが起動され（ステップ S108）、携帯電話機 50 とコンテンツサーバ 10a との間でパケット通信が開始される。そして、ユーザが操作入力部 505 を操作してダウンロードするプログラムを指定すると、このプログラムのダウンロードを要求する信号が携帯電話機 50 からコンテンツサーバ 10a へと送信される（ステップ S109）。コンテンツサーバ 10a は、ダウンロードの要求を受けたプログラムと、このプログラムの検査結果データ 202 とをメモリから読み出して携帯電話機 50 へ送信し（ステップ S110、S111）、携帯電話機 50 は、プログラムと検査結果データ 202 を受信すると、これらを不揮発性メモリ 507 に記憶する（ステップ S112）。

【0035】

次に、図 7 は、携帯電話機 50 において実行される、ネットワークを介して受信したプログラムの実行可否を判定する処理の動作を例示するフローチャートである。この処理は、携帯電話機 50 において、ネットワークを介して受信したプログラムを実行する旨が指示された場合に、CPU 501 により実行される。同図に示すように、まず、CPU 501 は、実行する旨が指示されたプログラムの検査結果データ 202 を不揮発性メモリ 507 から読み出す（ステップ S201）。

【0036】

次いで、CPU 501 は、読み出した検査結果データ 202 の電子署名を検証し（ステップ S202）、この検査結果データ 202 が検査機関 20 によって生成されたものであること、改竄等が行われていない正当な検査結果データ 202 であることを確認する。その結果、正当な検査結果データ 202 でないことが判った場合（ステップ S203：NO）、CPU 501 は、プログラムの実行を中止し（ステップ S210）、検査結果データ 202 に改竄等の不正が見つかったため、プログラムの実行を中止したことを示すメッセージを液晶画面に表示する。

【0037】

一方、正当な検査結果データ 202 であることが検証された場合（ステップ S203：YES）、CPU 501 は、検査結果データ 202 に記録されているハッシュアルゴリズムを用いて、実行する旨が指示されたプログラムのハッシュ値を算出する。次いで、CPU 501 は、算出したハッシュ値と、検査結果データ 202 に記録されているハッシュ値とを照合する（ステップ S204）。その結果、ハッシュ値が一致しなかった場合（ステップ S205：NO）、CPU 501 は、プログラムの実行を中止し（ステップ S210）、プログラムに改竄等の不正が見つかったため、プログラムの実行を中止したことを示すメッセージを表示する。

【0038】

また、ハッシュ値が一致した場合（ステップ S205：YES）、CPU 501 は、現時点において携帯電話機 50 に設定されているセキュリティレベルの値を特定し、特定したセキュリティレベルの値に対応するセキュリティ管理テーブル 507a を不揮発性メモリ 507 から読み出す（ステップ S206）。そして、CPU 501 は、読み出したセキュリティ管理テーブル 507a と、ステップ S201 において取得した検査結果データ 202 とを比較して（ステップ S207）、実行する旨が指示されたプログラムの実行可否を判定する（ステップ S208）。

【0039】

このステップ S207、S208 における処理について具体的に説明すると、まず、CPU501 は、検査結果データ 202 に記録されている各関数、すなわち、実行する旨が指示されたプログラムから抽出された各関数毎に、この関数がセキュリティ管理テーブル 507a において使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。同様に、CPU501 は、検査結果データ 202 に記録されている各リソース毎に、このリソースがセキュリティ管理テーブル 507a においてアクセスを許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。

【0040】

その結果、CPU501 は、使用が禁止された関数が検査結果データ 202 に 1 つでも記録されていた場合や、アクセスが禁止されたリソースが検査結果データ 202 に 1 つでも記録されていた場合に、実行する旨が指示されたプログラムは、ユーザによって設定されたセキュリティポリシー（セキュリティ管理テーブル 507a）に違反するものであると判断し、このプログラムの実行を許可しない（ステップ S208：NO）。この場合、CPU501 は、プログラムの実行を中止し（ステップ S210）、例えば、図 8 に示すようなメッセージを液晶画面に表示する。

【0041】

例えば、検査結果データ 202 が図 2 に示すものである一方、セキュリティ管理テーブル 507a が図 4 に示すものであった場合、検査結果データ 202 には、セキュリティ管理テーブル 507a において使用が禁止された関数“Function1 ()”や、セキュリティ管理テーブル 507a においてアクセスが禁止されたリソース“Local/UserData/Address Book”が記録されているから、この検査結果データ 202 が付与されているプログラムは、携帯電話機 50 において実行が許可されない。

【0042】

一方、CPU501 は、検査結果データ 202 に記録されている全ての関数がセキュリティ管理テーブル 507a において使用を許可された関数であって、かつ、検査結果データ 202 に記録されている全てのリソースがセキュリティ管理テーブル 507a においてアクセスを許可されたリソースであった場合に、実行する旨が指示されたプログラムは、ユーザによって設定されたセキュリティポリシーを満たすものであると判断し、このプログラムの実行を許可する（ステップ S208：YES）。この場合、CPU501 は、実行することが許可されたプログラムを不揮発性メモリ 507 から読み出して起動し（ステップ S209）、このプログラムに従った処理を開始する。

【0043】

なお、図 4 に示したセキュリティ管理テーブル 507a におけるリソース“http://www.xxx.co.jp”のように、「許可」の項目に“ユーザ確認”が登録されているリソースが検査結果データ 202 に記録されていた場合、CPU501 は、プログラムの実行可否をユーザに問い合わせるメッセージを生成して液晶画面に表示し、操作入力部 505 からの指示に従ってプログラムの実行可否を決定する。

【0044】

以上説明したように本実施形態によれば、プログラム検査装置 20a は、ネットワークを介して携帯電話機 50 に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ 202 を生成する。携帯電話機 50 は、ネットワークを介して受信したプログラムの実行可否を、このプログラムの検査結果データ 202 と、各関数についての使用許可や各リソースについてのアクセスの許可が登録されたセキュリティ管理テーブル 507a とを比較して判定する。したがって、携帯電話機 50 は、受信したプログラムを解析せずとも、検査結果データ 202 とセキュリティ管理テーブル 507a とを比較するだけで、このプログラムが携帯電話機 50 に設定されたセキュリティポリシー（セキュリティ管理テーブル 507a）を満たすプログラムであるか否かを判定することができる。よって、このような判定処理を携帯電話機 50 において簡易な構成で短時間

のうちに済ますことができる。

【0045】

また、受信したプログラムの実行可否を判定するために用いるセキュリティ管理テーブル507aは、セキュリティレベルを変更することによって容易に変更可能である。したがって、例えば、セキュリティポリシーに違反するとして実行が認められなかったプログラムであっても、ユーザ自身がこのプログラムは十分に信頼し得るものであると判断した場合は、一時的にセキュリティレベルを下げて、このプログラムを携帯電話機50において実行すること等が可能となる。このように本実施形態によれば、受信したプログラムに対する携帯電話機50のセキュリティを、ユーザの意向に応じて柔軟に設定することができるという効果も奏する。

【0046】

[B. 第2実施形態]

次に、本発明の第2実施形態について説明する。

なお、本実施形態において、第1実施形態と共通する部分については同一の符号を使用するものとする。また、第1実施形態と共通する部分についてはその説明を省略するものとする。

【0047】

図9は、コンテンツサーバ10aと携帯電話機50との間で行われるパケット通信を中継する中継装置60のハードウェア構成を例示するブロック図である。なお、この中継装置60は、インターネット30上に設けられていてもよいし、移動パケット通信網40に設けられていてもよい。同図において、通信インタフェース604は、CPU601の制御の下、コンテンツサーバ10aや携帯電話機50との間で行われるパケット通信を制御する。操作入力部605は、キーボードやマウスを備え、これらの操作に応じた操作信号をCPU601に出力する。表示部606は、LCDやCRTディスプレイ等である。

【0048】

HD(ハードディスク)607には、第1実施形態において説明したセキュリティ管理テーブル507aが記憶されている。本実施形態における中継装置60は、このセキュリティ管理テーブル507aを用いて、コンテンツサーバ10aから携帯電話機50に宛てて送信されたプログラムの中継可否を判定する。なお、中継装置60は、コンテンツサーバ10aからプログラムとともに、このプログラムの検査結果データ202と、このプログラムの送信先を示す宛先情報とを受信するが、検査結果データ202は、第1実施形態において説明したプログラム検査装置20aによって生成されたものである。また、宛先情報は、例えばIPアドレス等の、携帯電話機50に対して割り当てられた通信アドレスである。

【0049】

また、本実施形態においては、移動パケット通信網40の通信事業者や中継装置60の管理者等によって、中継装置60に対し、セキュリティレベルが設定される。HD607には、第1実施形態において説明したように、セキュリティレベル毎に異なるセキュリティ管理テーブル507aが記憶されており、中継装置60に対して設定されたセキュリティレベルによって、プログラムの中継可否を判定する際に用いるセキュリティ管理テーブル507aが決定される。

【0050】

図10は、中継装置60において実行される、プログラムの中継可否を判定する処理の動作を例示するフローチャートである。この処理は、コンテンツサーバ10aから携帯電話機50に宛てて送信されたプログラムとその検査結果データ202を中継装置60が受信した場合に、CPU601により実行される。同図に示すように、まず、CPU601は、受信した検査結果データ202の電子署名を検証する(ステップS301)。その結果、CPU601は、正当な検査結果データ202でないことが判った場合(ステップS302:NO)、携帯電話機50に対するプログラムの転送を中止し(ステップS309)、プログラムに付与されている検査結果データ202に改竄等の不正が見つかったため

、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機 50 へ送信する。

【0051】

一方、正当な検査結果データ 202 であることが検証された場合（ステップ S302: YES）、CPU601 は、検査結果データ 202 に記録されているハッシュアルゴリズムを用いて、受信したプログラムのハッシュ値を算出し、検査結果データ 202 に記録されているハッシュ値と照合する（ステップ S303）。その結果、CPU601 は、ハッシュ値が一致しなかった場合（ステップ S304: NO）、携帯電話機 50 に対するプログラムの転送を中止し（ステップ S309）、プログラムに改竄等の不正が見つかったため、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機 50 へ送信する。

【0052】

また、ハッシュ値が一致した場合（ステップ S304: YES）、CPU601 は、現時点において中継装置 60 に設定されているセキュリティレベルの値を特定し、特定したセキュリティレベルの値に対応するセキュリティ管理テーブル 507a を HD607 から読み出す（ステップ S305）。そして、CPU601 は、読み出したセキュリティ管理テーブル 507a と、受信した検査結果データ 202 とを比較して（ステップ S306）、携帯電話機 50 に対するプログラムの中継可否を判定する（ステップ S307）。

【0053】

このステップ S306、S307 における処理について具体的に説明すると、まず、CPU601 は、検査結果データ 202 に記録されている各関数、すなわち、受信したプログラムから抽出された各関数毎に、この関数がセキュリティ管理テーブル 507a において使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。同様に、CPU601 は、検査結果データ 202 に記録されている各リソース毎に、このリソースがセキュリティ管理テーブル 507a においてアクセスを許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。

【0054】

その結果、CPU601 は、使用が禁止された関数が検査結果データ 202 に 1 つでも記録されていた場合や、アクセスが禁止されたリソースが検査結果データ 202 に 1 つでも記録されていた場合に、転送されてきたプログラムは、移動パケット通信網 40 の通信事業者等によって設定されたセキュリティポリシー（セキュリティ管理テーブル 507a）に違反するものであると判断し、このプログラムの携帯電話機 50 への中継を許可しない（ステップ S307: NO）。この場合、CPU601 は、プログラムの転送を中止し（ステップ S309）、セキュリティポリシーに違反するプログラムであったため、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機 50 へ送信する。

【0055】

一方、CPU601 は、検査結果データ 202 に記録されている全ての関数がセキュリティ管理テーブル 507a において使用を許可された関数であって、かつ、検査結果データ 202 に記録されている全てのリソースがセキュリティ管理テーブル 507a においてアクセスを許可されたリソースであった場合に、転送されてきたプログラムは、通信事業者等によって設定されたセキュリティポリシーを満たすものであると判断し、このプログラムの携帯電話機 50 への中継を許可する（ステップ S307: YES）。この場合、CPU601 は、宛先情報によって示される携帯電話機 50 へプログラムを転送する（ステップ S308）。

【0056】

以上説明したように本実施形態によれば、プログラム検査装置 20a は、ネットワークを介して携帯電話機 50 に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ 202 を生成する。中継装置 60 は、携帯電話機 50 に対するプログラムの中継可否を、このプログラムの検査結果データ 202 と、各関数につい

ての使用許可や各リソースについてのアクセスの許可が登録されたセキュリティ管理テーブル507aとを比較して判定する。したがって、中継装置60は、転送するプログラムを解析せずとも、検査結果データ202とセキュリティ管理テーブル507aとを比較するだけで、このプログラムが中継装置60に設定されたセキュリティポリシー（セキュリティ管理テーブル507a）を満たすプログラムであるか否かを判定することができる。よって、このような判定処理を中継装置60において簡易な構成で短時間のうちに済ますことができ、通信の遅延を招いたり、通信網のトラフィックに支障をきたすようなことがない。また、セキュリティポリシーに違反するプログラムについては転送を中止するから、携帯電話機50への提供を未然に防ぐことができる。

【0057】

なお、セキュリティ管理テーブル507aに登録する関数や、各関数についての使用の許可は、移動パケット通信網40の通信事業者や中継装置60の管理者等によって任意に変更可能である。勿論、セキュリティ管理テーブル507aに登録するリソースや、各リソースについてのアクセスの許可についても同様である。

【0058】

[C. 変形例]

(1) 第1実施形態では、検査結果データ202がプログラムに付与されて携帯電話機50へ送信されてくる場合について説明した。しかしながら、図11に示すように、検査結果登録サーバ70を設け、この検査結果登録サーバ70に、検査機関20において検査された各プログラムの検査結果データ202が登録される構成としてもよい。この場合、携帯電話機50は、コンテンツサーバ10bからプログラムをダウンロードした後に、このプログラムの検査結果データ202を検査結果登録サーバ70から取得する。また、第2実施形態についても同様であって、検査結果登録サーバ70に各プログラムの検査結果データ202が登録され、中継装置60は、携帯電話機50へ転送するプログラムをコンテンツサーバ10bから受信すると、このプログラムの検査結果データ202を検査結果登録サーバ70から取得するようにしてもよい。なお、検査結果登録サーバ70は、移動パケット通信網40に設けられていてもよいし、検査機関20内に設けられていてもよい。

【0059】

(2) 第1実施形態において、図7に示したフローチャートのステップS208にてNOと判定された場合以降の処理を、図12に示すように変形してもよい。

すなわち、CPU501は、図7のステップS208にてNOと判定された場合に、まず、図13に示すように、実行する旨が指示されたプログラムがセキュリティポリシーに違反していることと、使用可能な機能を制限した上でこのプログラムを実行するか否かを問い合わせるメッセージを液晶画面に表示する（ステップS401）。このメッセージの表示に応じてユーザは、使用可能な機能を制限してプログラムを実行することとするのか、それともプログラムの実行を中止するかを、操作入力部505を操作して携帯電話機50に指示する。なお、上記メッセージは、音声メッセージとして携帯電話機50から出力されてもよい。

【0060】

CPU501は、プログラムの実行を中止する旨が操作入力部505から指示された場合（ステップS402：NO）、プログラムの実行を中止する（ステップS403）。一方、CPU501は、プログラムを実行する旨が操作入力部505から指示された場合（ステップS402：YES）、実行する旨が指示されたプログラムを不揮発性メモリ507から読み出して起動する（ステップS404）。次いで、CPU501は、プログラムの実行が終了したか否かを判別し（ステップS405）、プログラムの実行が終了するまでの間、このプログラムにおいて使用可能な機能を、セキュリティ管理テーブル507aに従って制限する（ステップS406）。なお、使用可能な機能を制限する際に用いるセキュリティ管理テーブル507aは、現時点において携帯電話機50に設定されているセキュリティレベルに対応するものである。

【0061】

このステップS406における処理について具体的に説明すると、まず、CPU501は、プログラムを順次解釈して実行していく際に、ファンクションコール、システムコール、機能呼び出し等の関数があった場合、この関数がセキュリティ管理テーブル507aにおいて使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。そして、CPU501は、使用が許可された関数であった場合に、この関数の使用を許可してプログラムの実行を継続する一方、使用が禁止された関数であった場合は、この関数の使用を許可せず、プログラムの実行を中止する。

【0062】

また、CPU501は、プログラムを順次解釈して実行していく過程で発生する、各種リソースへのアクセス要求を監視し、アクセス要求のあったリソースがセキュリティ管理テーブル507aにおいてアクセスが許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。そして、CPU501は、アクセスが許可されたリソースであった場合に、このリソースに対するアクセスを許可してプログラムの実行を継続する一方、アクセスが禁止されたリソースであった場合は、このリソースに対するアクセスを許可せず、プログラムの実行を中止する。

【0063】

以上説明した構成とすれば、携帯電話機50では、セキュリティポリシーに違反するプログラムであっても、使用可能な機能を制限した上でこのプログラムを実行することができる。

【0064】

(3) セキュリティ管理テーブル507aには、使用が許可された関数と使用が禁止された関数の情報のみが登録されていてもよい。また、逆に、アクセスが許可されたリソースとアクセスが禁止されたリソースの情報のみがセキュリティ管理テーブル507aに登録されていてもよい。さらに、使用が許可された関数の情報のみ、あるいは使用が禁止された関数の情報のみがセキュリティ管理テーブル507aに登録されていてもよいし、アクセスが許可されたリソースの情報のみ、あるいはアクセスが禁止されたリソースの情報のみがセキュリティ管理テーブル507aに登録されていてもよい。

【0065】

(4) 第2実施形態において、中継装置60のHD607には、各携帯電話機50毎に、携帯電話機50のユーザによって設定されたセキュリティレベルが登録されるようにして、中継装置60では、プログラムの転送先となる携帯電話機50のセキュリティレベルを特定し、このセキュリティレベルに対応するセキュリティ管理テーブル507aを用いてプログラムの中継可否を判定するようにしてもよい。

【0066】

(5) 第1実施形態において、携帯電話機50の不揮発性メモリ507には、さらに、検査結果表202が付与されていないプログラムについて、その実行可否を判定するために用いるセキュリティ管理テーブルが記憶されていてもよい。また、検査機関20と同様の検査機関が複数ある場合に、検査機関20とは別の検査機関によって生成された検査結果データが付与されているプログラムについて、その実行可否を判定するために用いるセキュリティ管理テーブルが不揮発性メモリ507に記憶されていてもよい。これは、第2実施形態における中継装置60についても同様であって、HD607には、検査結果表202が付与されていないプログラムや、検査機関20とは別の検査機関によって生成された検査結果データが付与されているプログラムについて、その中継可否を判定するために用いるセキュリティ管理テーブルが記憶されていてもよい。

【0067】

(6) 第1実施形態において、検査結果データ202には、コンテンツプロバイダの名称やプログラムの送信元を示すURL等、プログラムの提供元を識別するための提供者識別情報をさらに記録するようにして、携帯電話機50の不揮発性メモリ507には、提供者識別情報毎に異なるセキュリティ管理テーブル507aを記憶しておき、携帯電話機50は、受信した検査結果データ202に記録されている提供者識別情報に対応するセキュリ

ティ管理テーブル 5 0 7 a を用いて、受信したプログラムの実行可否を判定するようにしてもよい。第 2 実施形態についても同様であって、検査結果データ 2 0 2 には、提供者識別情報をさらに記録するようにして、中継装置 6 0 の H D 6 0 7 には、提供者識別情報毎に異なるセキュリティ管理テーブル 5 0 7 a を記憶しておき、中継装置 6 0 は、受信した検査結果データ 2 0 2 に記録されている提供者識別情報に対応するセキュリティ管理テーブル 5 0 7 a を用いて、プログラムの中継可否を判定するようにしてもよい。

【0068】

(7) 第 1 実施形態において、携帯電話機 5 0 は、プログラムがダウンロードされたときに、このプログラムの検査結果データ 2 0 2 とセキュリティ管理テーブル 5 0 7 a とを比較して、このプログラムがセキュリティポリシー（セキュリティ管理テーブル 5 0 7 a）を満たすプログラムであるか否かを判定し、その判定結果を液晶画面に表示するようにしてもよい。勿論、判定結果は、音声メッセージとして携帯電話機 5 0 から出力されてもよい。また、携帯電話機 5 0 は、受信したプログラムについてユーザが操作入力部 5 0 5 を操作してその安全性を検証するよう指示したときに、指示されたプログラムの検査結果データ 2 0 2 とセキュリティ管理テーブル 5 0 7 a とを比較して、このプログラムがセキュリティポリシーを満たすプログラムであるか否かを判定し、その判定結果を出力するようにしてもよい。

【0069】

このように、ネットワークを介して受信したプログラムについて、実行の可否を判定するのではなく、セキュリティポリシーを満たすプログラムであるか否かを判定し、その判定結果をユーザに報知する構成としてもよい。この場合、ユーザは、報知された判定結果に従って、セキュリティポリシーに違反するプログラムであった場合は、このプログラムを不揮発性メモリ 5 0 7 から削除（アンインストール）したり、実行しないようにすることができ、携帯電話機 5 0 のセキュリティを保つことができる。なお、セキュリティポリシーに違反するプログラムであった場合は、このプログラムに含まれていた、使用することが許可されていない関数の名称や、アクセスすることが許可されていないリソースを示す情報を、判定結果とともにユーザに報知する構成としてもよい。また、セキュリティポリシーに違反するプログラムであった場合は、このプログラムを削除するか否かを問うメッセージを液晶画面に表示し、操作入力部 5 0 5 から削除する旨が指示された場合に、このプログラムを不揮発性メモリ 5 0 7 からアンインストールする構成としてもよい。

【0070】

また、第 2 実施形態において中継装置 6 0 は、携帯電話機 5 0 へプログラムを転送するときに、転送するプログラムの検査結果データ 2 0 2 と、セキュリティ管理テーブル 5 0 7 a とを比較して、このプログラムがセキュリティポリシー（セキュリティ管理テーブル 5 0 7 a）を満たすプログラムであるか否かを判定し、その判定結果をプログラムとともに携帯電話機 5 0 へ送信するようにしてもよい。

【0071】

(8) 第 1 実施形態における携帯電話機 5 0 を以下のように変形してもよい。

すなわち、携帯電話機 5 0 は、コンテンツサーバ 1 0 a からプログラムをダウンロードする前に、まず、ダウンロードするプログラムの検査結果データ 2 0 2 のみをコンテンツサーバ 1 0 a から受信する。次いで、携帯電話機 5 0 は、受信した検査結果データ 2 0 2 とセキュリティ管理テーブル 5 0 7 a とを比較して、ダウンロードしようとしているプログラムが、セキュリティポリシー（セキュリティ管理テーブル 5 0 7 a）を満たすプログラムであるか否かを判定する。その結果、携帯電話機 5 0 は、セキュリティポリシーを満たすプログラムであった場合は、このプログラムをコンテンツサーバ 1 0 a からダウンロードする一方、セキュリティポリシーに違反するプログラムであった場合は、このプログラムのダウンロードを中止する。このような構成とすれば、セキュリティポリシーに違反するプログラムであった場合には、このプログラムのダウンロードを事前に中止することができるから、無駄なパケット通信を行わずに済む。

【0072】

(9) 第1および第2実施形態では、プログラムをダウンロードする場合について説明したが、勿論、プログラムを携帯電話機50に配信する場合についても本発明を適用することができる。また、本発明に係る受信装置を、公衆無線LANを介して通信を行う無線端末や、インターネットを介して通信を行うパーソナルコンピュータ等に適用してもよい。また、本発明に係る中継装置を、ゲートウェイサーバやプロキシサーバ、移動パケット通信網40に設けられた交換局や基地局等に適用してもよい。また、本発明に係る処理を携帯電話機50や中継装置60等のコンピュータに実行させるためのプログラムは、通信によってコンピュータにインストールされてもよい。また、コンピュータによって読み取り可能な各種の記録媒体に上記プログラムを記録して頒布してもよい。

【図面の簡単な説明】

【0073】

【図1】 第1実施形態に係る通信システム1の構成を例示するブロック図である。

【図2】 同実施形態に係り、検査結果データ202のデータ構成を例示する図である。

【図3】 同実施形態に係り、携帯電話機50のハードウェア構成を例示するブロック図である。

【図4】 同実施形態に係り、セキュリティ管理テーブル507aのデータ構成を例示する図である。

【図5】 同実施形態に係り、プログラムとその検査結果データ202が携帯電話機50にダウンロードされるまでの通信システム1各部の動作について例示するシーケンスチャートである。

【図6】 同実施形態に係り、セキュリティレベルを設定する際の携帯電話機50の画面表示例を示す図である。

【図7】 同実施形態に係り、携帯電話機50において実行される、ネットワークを介して受信したプログラムの実行可否を判定する処理の動作を例示するフローチャートである。

【図8】 同実施形態に係り、プログラムの実行が許可されなかった場合の携帯電話機50の画面表示例を示す図である。

【図9】 第2実施形態に係り、中継装置60のハードウェア構成を例示するブロック図である。

【図10】 同実施形態に係り、中継装置60において実行される、プログラムの中継可否を判定する処理の動作を例示するフローチャートである。

【図11】 変形例(1)に係る通信システム2の構成を例示するブロック図である。

【図12】 変形例(2)に係る携帯電話機50において実行される処理の動作を例示するフローチャートである。

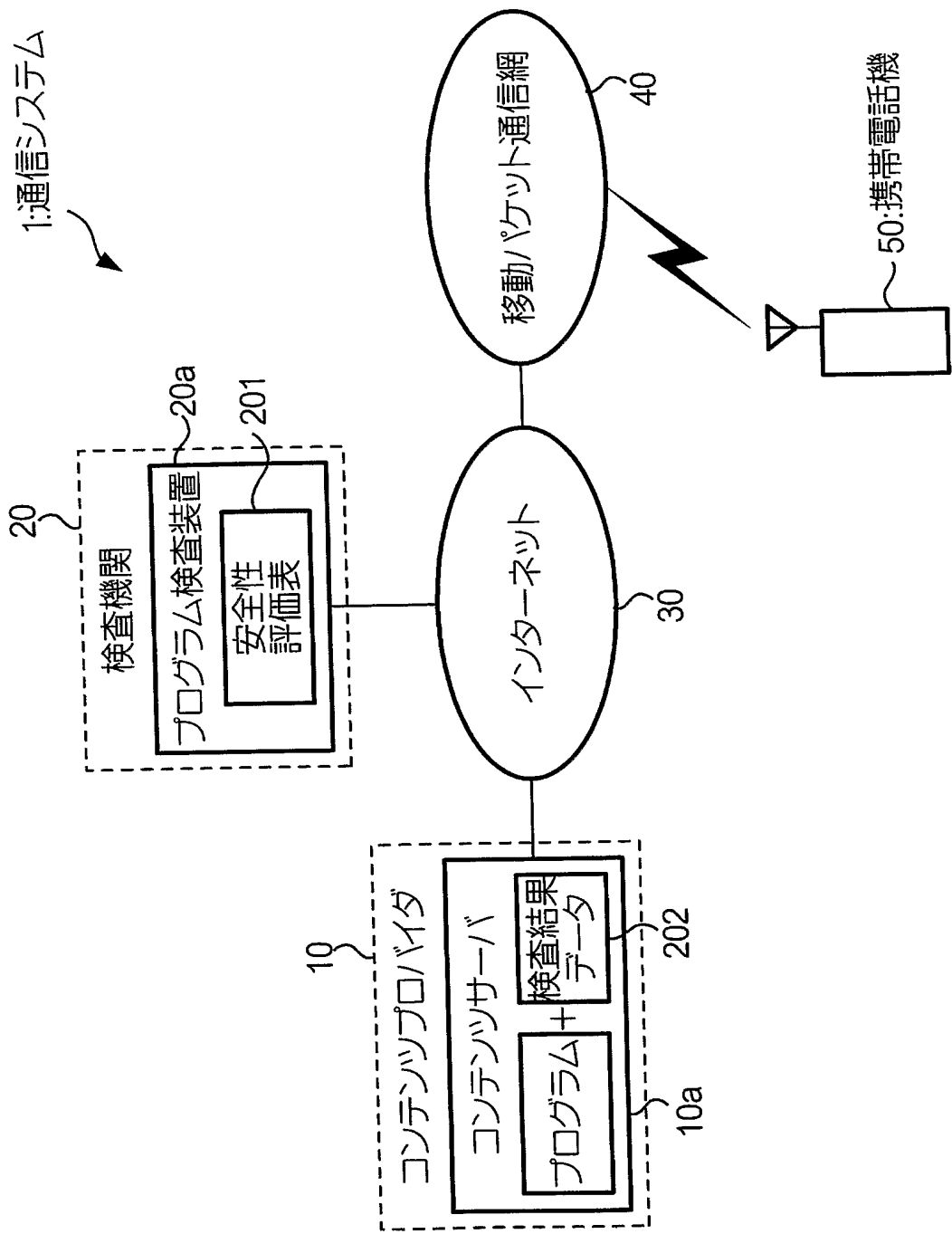
【図13】 変形例(2)に係る携帯電話機50の画面表示例を示す図である。

【符号の説明】

【0074】

1, 2…通信システム、10…コンテンツプロバイダ、10a, 10b…コンテンツサーバ、20…検査機関、20a…プログラム検査装置、30…インターネット、40…移動パケット通信網、50…携帯電話機、60…中継装置、70…検査結果登録サーバ、201…安全性評価表、202…検査結果データ、501…CPU、502…ROM、503…RAM、504…無線通信部、505…操作入力部、506…液晶表示部、507…不揮発性メモリ、507a…セキュリティ管理テーブル、601…CPU、602…ROM、603…RAM、604…通信インタフェース、605…操作入力部、606…表示部、607…HD。

【書類名】 図面
【図 1】

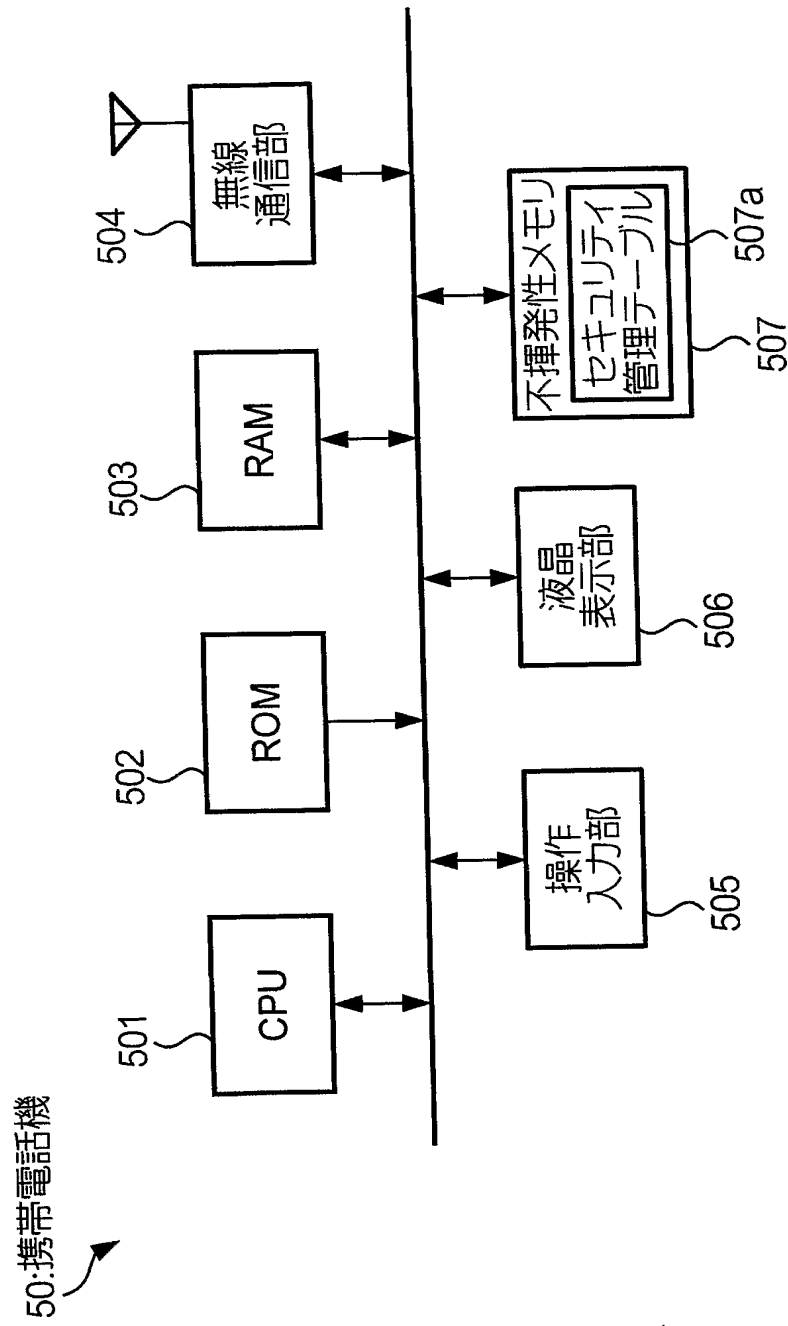


【図 2】

202:検査結果データ

プログラム	Sample.APP	
ハッシュアルゴリズム	MD5	
ハッシュ値	0D247FCB001A2BC5FED000009355FF23	
関数	関数名	
	Function 1 ()	
	Function 2 ()	
	Function 5 ()	
	⋮	
アクセス先リソース	タイプ	リソース
	Network	http://www.xxx.co.jp
	File	Local/UserData/AddressBook
	⋮	⋮

【図 3】

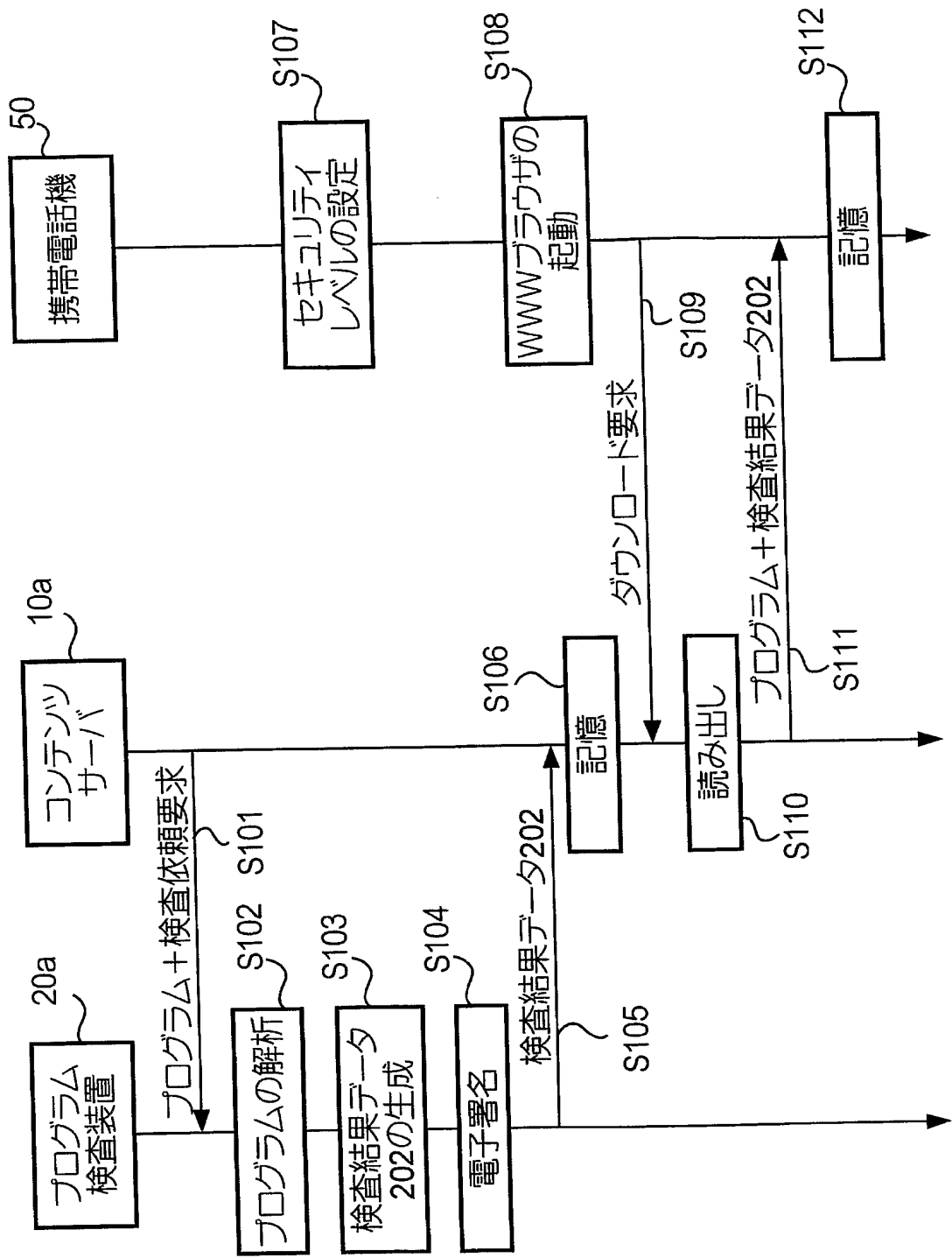


【図 4】

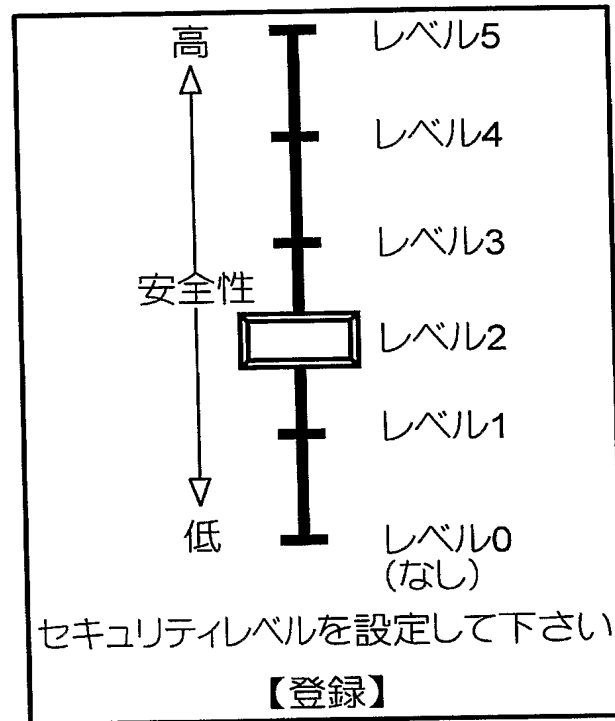
507a:セキュリティ管理テーブル

セキュリティレベル	レベル1	カテゴリ	関数名	可否
関数		ファイルアクセス	Function 1 ()	禁止
			Function 2 ()	許可
		ネットワークアクセス	全ての関数	禁止
		⋮	⋮	⋮
		タイプ	リソース	可否
アクセス先リソース		Network	http://www.xxx.co.jp	ユーザ確認
		DataFile	全てのデータファイル	禁止
		File	Local/UserData/AddressBook	禁止
		⋮	⋮	⋮

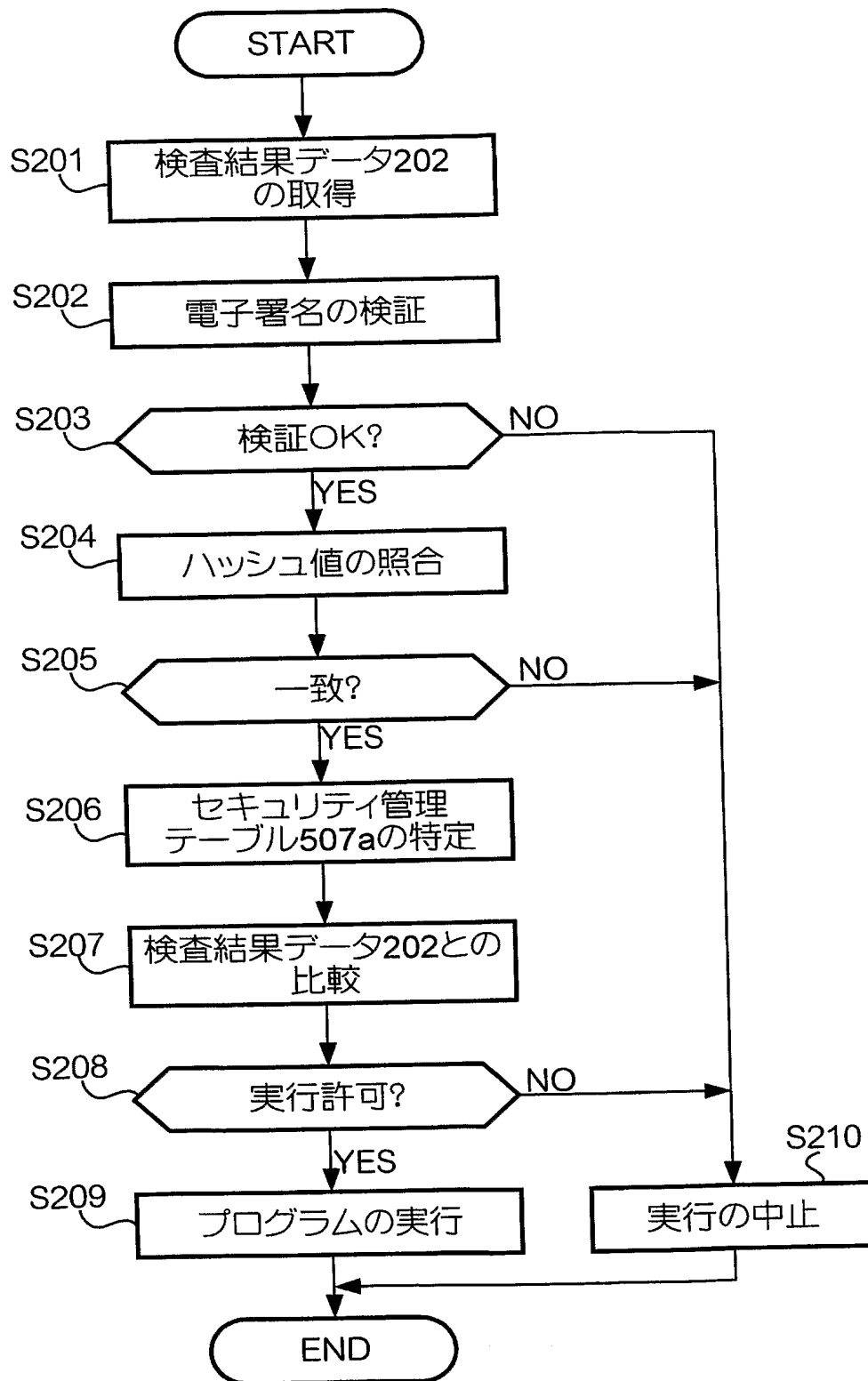
【図 5】



【図 6】



【図 7】



【図 8】

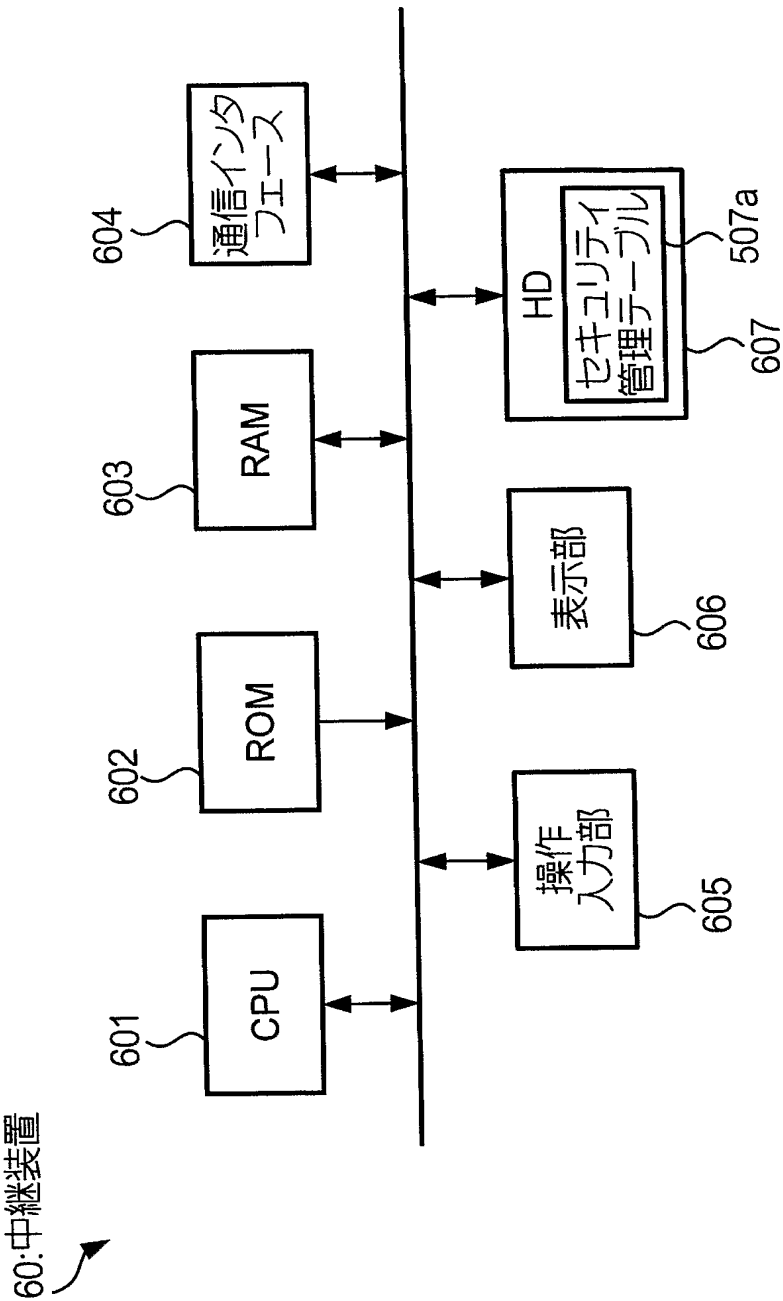
警告

このプログラムは、あなたが設定したセキュリティポリシーに違反しているため、実行を中止します。

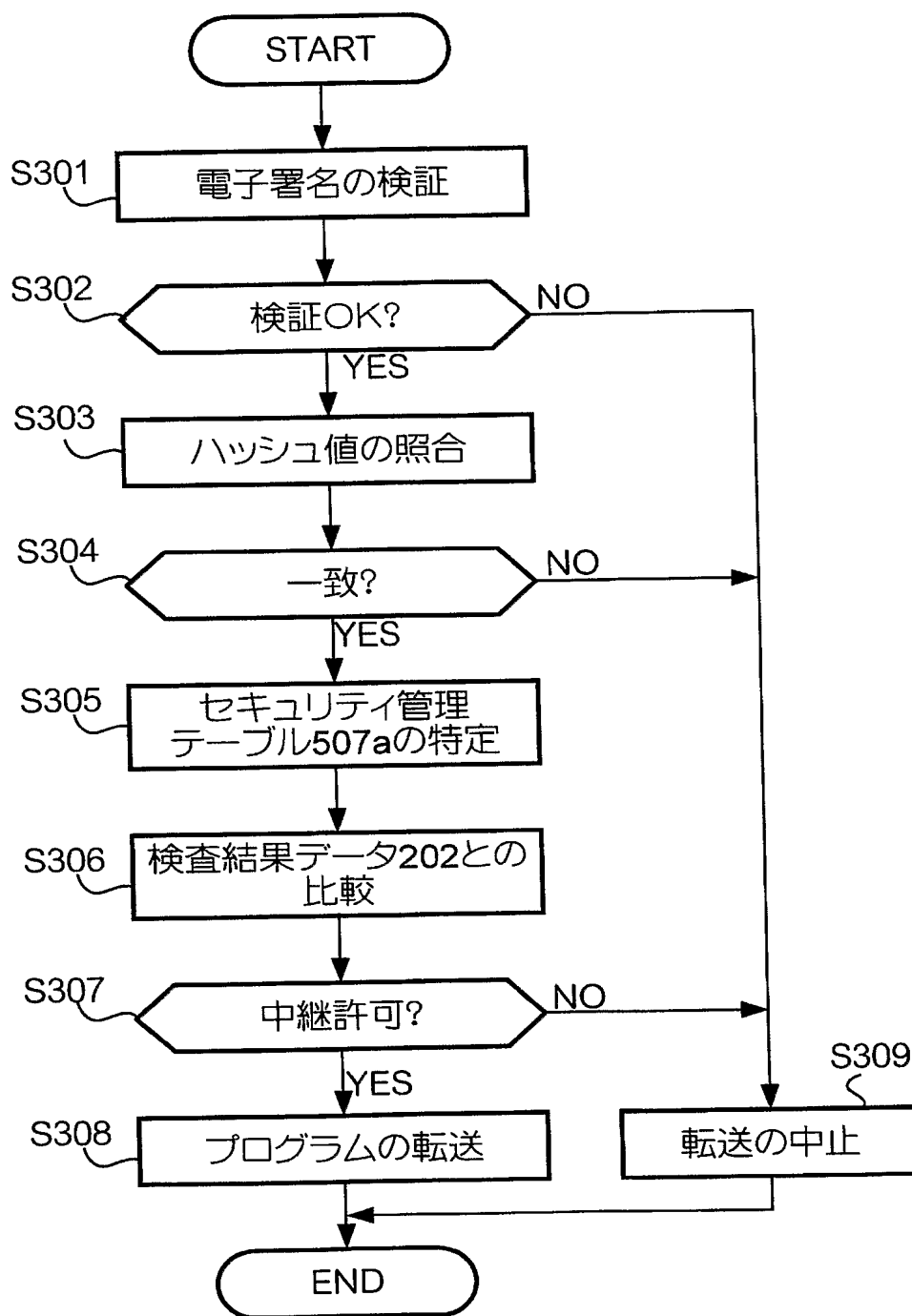
【戻る】

【セキュリティポリシーの確認】

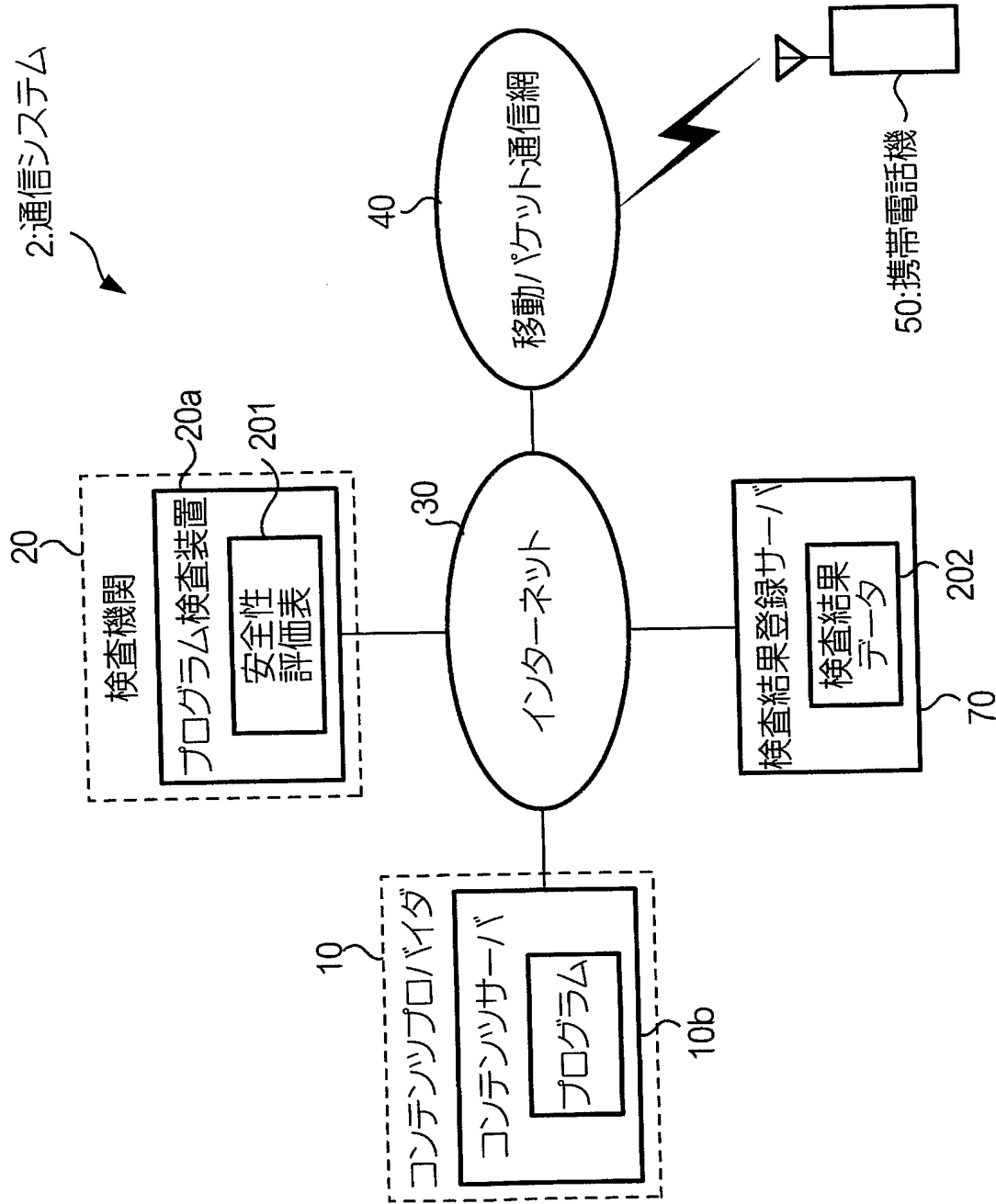
【図 9】



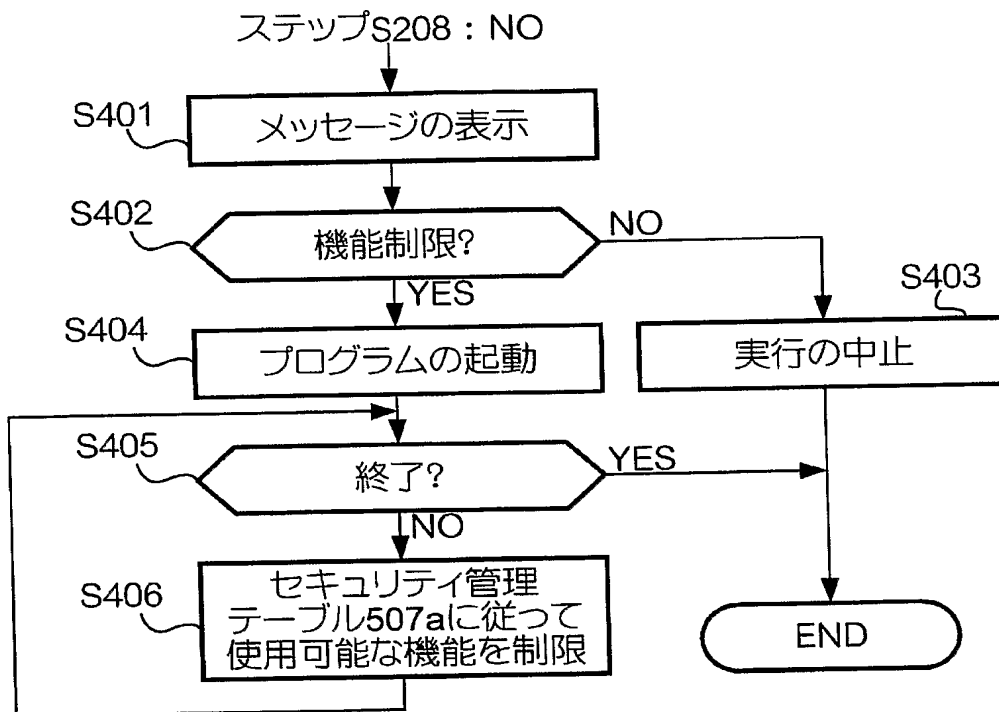
【図 10】



【図 11】



【図 12】



【図 13】

このプログラムは、セキュリティポリシーに違反しています。
使用可能な機能を制限して
プログラムを実行しますか？

【実行】 【中止】

【書類名】 要約書**【要約】**

【課題】 ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定できるようにすること。

【解決手段】 プログラム検査装置 20 a は、ネットワークを介して携帯電話機 50 に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ 202 を生成する。携帯電話機 50 は、各関数についての使用許否や、各リソースについてのアクセスの許否が登録されたセキュリティ管理テーブル 507 a を有しており、ネットワークを介して受信したプログラムについて、このプログラムの検査結果データ 202 と、セキュリティ管理テーブル 507 a とを比較して、このプログラムを実行した場合にセキュリティ上の問題が起きないか判定する。

【選択図】 図 1

【書類名】 手続補正書
【提出日】 平成16年12月 2日
【あて先】 特許庁長官 殿
【事件の表示】
【出願番号】 特願2004- 29928
【補正をする者】
【識別番号】 397011166
【氏名又は名称】 トレンドマイクロ株式会社
【代理人】
【識別番号】 100098084
【弁理士】
【氏名又は名称】 川▲崎▼ 研二
【電話番号】 03-3242-5481
【手続補正1】
【補正対象書類名】 特許願
【補正対象項目名】 発明者
【補正方法】 変更
【補正の内容】
【発明者】
【住所又は居所】 東京都渋谷区代々木 2 - 1 - 1 トレンドマイクロ株式会社内
【氏名】 近藤 賢志
【発明者】
【住所又は居所】 東京都渋谷区代々木 2 - 1 - 1 トレンドマイクロ株式会社内
【氏名】 谷田部 茂
【その他】 平成16年2月5日付出願の特願2004-29928号の特許願の発明者の氏名を「近藤 賢志」「谷田部 茂」と記するところを誤って「近藤 賢志」「矢田部 茂」として出願してしまいました。上記氏名の誤記を訂正いたしたく本書を提出致しますので、宜しくお願い申し上げます。

特願 2 0 0 4 - 0 2 9 9 2 8

出 願 人 履 歴 情 報

識別番号

[3 9 7 0 1 1 1 6 6]

1. 変更年月日

2 0 0 3 年 1 1 月 2 6 日

[変更理由]

住所変更

住 所

東京都渋谷区代々木 2 - 1 - 1 新宿マインズタワー

氏 名

トレンドマイクロ株式会社